futuro
0100010100100010010001010100011
Año 15 / N° 785 | 13 . 03 . 2004

CRIPTOGRAFIA

Juegos de guerra

Durante miles de años, desde el antiguo Egipto a la era de Internet, la comunicación eficiente ha sido el eslabón dorado que amalgamó reinos, imperios y repúblicas. Que ciertos mensajes cayeran en las manos equivocadas, sacando a la luz los más oscuros secretos del poder, significaba capitular ante un enemigo siempre al acecho. Así nacieron los códigos y las cifras, técnicas varias para proteger y descifrar mensajes de forma que sólo puedan ser leídos por el receptor a quien originariamente iban dirigidos. Hay códigos que han decidido el desenlace de batallas, vida y muerte de reyes y reinas, además de dar un fuerte empujón al desarrollo de las computadoras, en un siempre presente clima de intrigas políticas y disputas ideológicas. No por nada conocer es poder.

POR GUILLERMO MOVIA

En 1940, G. H. Hardy, matemático inglés, escribió: "La matemática real no tiene efectos en la guerra. Nadie ha descubierto aún ningún propósito belicoso al que pueda servir la teoría de los números". Treinta años más tarde, uno de sus discípulos hizo un descubrimiento que lo desmentiría: la función que permitía hacer de las cifras un arma de guerra, usando solamente un par de números primos. Años después, con la rapidez de cálculo que ofrecen las computadoras, los mensajes digitales pueden ser protegidos de cualquier intento de escucha o lectura indeseada, incluso un plan de ataque terrorista o la compra de un compact disc por Internet.

EL CIFRADO

Cifrar es proteger un mensaje con una clave para que sólo pueda ser leído por determinadas personas. Los métodos más simples pueden ser practicados por chicos de primaria o conseguirse en cualquier revista de entretenimientos, en los cuales cada letra del alfabeto es reemplazada por otra, por un número o por un dibujo; siempre el mismo. De esta manera, basta con conocer el código para poder leerlo. Por ejemplo, una clave donde la letra "A" es reemplazada por la "X", la letra "B" por la "Y" y así sucesivamente. Simple.

Tan simple que es insegura para enviar mensajes importantes. Basta con un par de técnicas estadísticas para sacar a la luz los mensajes escondidos. Sin embargo, Julio César utilizó un sistema similar para avisarles a Cicerón y sus soldados, sitiados por las tropas galas, que los refuerzos se encontraban en camino. Por eso se conoce a este tipo de cifrado como "La cifra César".

El secreto siempre fue un arma poderosa. Dos milenios más tarde, la Segunda Guerra Mundial fue un terreno perfecto para la exploración en este campo y los matemáticos más importantes de cada bando estuvieron dedicados a desarrollar algún método que resultara inquebrantable (ver recuadro).

Pero siempre había un problema: ¿cómo lograr el intercambio de la clave sin arriesgarse a que caiga en poder del enemigo? Si una persona "A" quiere enviarle mensajes cifrados a su amigo "B", basta con que se encuentren en algún lugar para que intercambien el código con el que después van a codificar los envíos. Pero, ¿cómo hacerles llegar de forma segura la clave a quienes se encuentran lejos? ¿Cómo lograr de forma segura que la clave le llegue al capitán de un submarino que patrulla las costas del enemigo?



DIALOGO CON LA BIOLOGA MARIA LAURA GUICHON

Invasión

POR FEDERICO KUKSO

Hay veces que una ardilla es sólo eso, una ardilla. Pero cuando estos animalitos, simpáticos y movedizos, se mudan (o más bien, los mudan) a una zona no contemplada para ellos y devienen plaga invasiva, se convierten en un grave problema. Es el caso de la ardilla de panza roja (*Callosciurus erythraeus*), introducida en la Argentina hace 30 años, y hoy considerada una importante amenaza para la biodiversidad y el equilibrio del ecosistema pampeano. Pero no todo está perdido: hay científicos, como la bióloga María Laura Guichón (investigadora y profesora en la Universidad de Luján y en la Universidad de Buenos Aires, y flamante ganadora de una de las becas L'Oréal-Unesco for Women in Science 2004), que pasan horas y horas metidos en el campo, investigando su comportamiento y maneras de propagación. En diálogo con **Futuro**, la doctora Guichón explicó por qué esta ardilla merece tanta atención y qué se puede hacer para detenerla.

–¿Cómo surgió su interés por la ardilla de panza roja?

–Todo empezó cuando estaba haciendo mi tesis de doctorado en la Universidad de Luján, en mi trabajo de campo con coipos (nutrias). En ese lugar –la localidad de Jáuregui, donde se liberaron hace 30 años cinco individuos, que se trajeron como mascota porque son lindos y simpáticos– veía a estas ardillas todo el tiempo. Me parece que es un problema muy importante de analizar porque no se sabe casi nada de esta especie y porque entra en el marco de las invasiones biológicas, o sea, cuando una especie es originaria de determinado lugar (en este caso, el sudeste de Asia) y de repente aparece en otra zona, a donde no habría llegado por sus propios medios. A veces estos individuos no encuentran las condiciones apropiadas y mueren. Y en otros casos, se propagan, como pasó con la ardilla de panza roja, que encuentran alimento para nidificar, establecerse y reproducirse. Estas ardillas son chiquitas con cola larga, viven y anidan en los árboles y se alimenta de sus frutos.


M. L. GUICHON, GANADORA BECA L´OREAL 2004.

–¿Este tipo de invasión biológica se acrecentó con la globalización?

–No, esto pasa desde que el hombre es hombre. La historia humana está acompañada de movimientos de especies de un lado al otro. Lo que pasa es que ahora se hacen más estudios de qué puede pasar si alguien ingresa una especie nueva a un lugar y los estragos que puede realizar.

–¿Qué tipo de pérdidas económicas provoca esta ardilla?

–Todavía no hay estudios sistemáticos hechos sobre la especie. Entonces, no está debidamente cuantificado cuál es la pérdida que un productor tiene o los habitantes de la región tienen por la presencia de la ardilla. Lo que sí sabemos, a través de entrevistas que vengo realizando desde hace un año, es que hay muchas quejas, pero básicamente por dos motivos: una de los productores que tienen forestaciones o frutales porque las ardillas les comen todas las frutas. El otro tema del que se queja la gente es que las ardillas muerden y rompen el plástico que recubre los cables de electricidad, de televisión y los sistemas de riego.

–¿Qué tipo de trabajo hizo hasta ahora?

–Recién estoy comenzando. Lo que estamos haciendo es tratar de confeccionar un mapa de la distribución actual de la ardilla porque no se sabe hasta dónde llegó por el momento. Por eso realizamos entrevistas a los dueños de los campos y a los que viven en zonas rurales y urbanas de la región, para ver si ven o si tienen ardillas en sus lugares de residencia; y también estamos trabajando un poco con la percepción que tiene la gente del tema. Hay quienes ni siquiera saben que está en la zona. En cambio, los que tienen problemas no las quieren para nada, las consideran un problema para sus plantaciones. También estamos haciendo observaciones de comportamiento, qué es lo que come y por dónde se mueve. Todo está orientado a tratar de frenar el avance, que no siga colonizando áreas nuevas (por ejemplo, el Delta) y ver qué elementos del ambiente facilitan a la ardilla para que vaya conquistando áreas nuevas.

–¿Qué se puede hacer para detenerla?

–Dos cosas: una son acciones concretas para frenar el avance de la ardilla. Y otra, que la gente tome conciencia de que no es gratis estar llevando un animal de un lado al otro. Eso después puede dar origen a una nueva población, crear un nuevo foco de invasión y convertirse en una de las principales amenazas a la biodiversidad y al funcionamiento de los ecosistemas. Porque al introducirse una especie en un sistema natural que no la contenía hasta el momento, empieza a interactuar con los demás componentes del sistema, empieza a alimentarse y a competir con los demás animales. Y es imposible que no cambie nada si de golpe se tiene una especie nueva, y bastante abundante.

–¿En qué consiste la beca que ganó?

–Voy a ir por un año a la Universidad de Southampton (Gran Bretaña) y voy a estudiar el proceso de invasión de la ardilla trabajando con unos modelos matemáticos que simulan la dinámica de la población de ardillas, es decir, cómo se comporta esta población. Para eso se usan datos de las características biológicas de la especie y del ambiente. Mi idea es detectar cuáles son las vías que está usando para avanzar.

–¿Y después?

–La idea es volver con una propuesta de un plan de manejo para ver qué acciones se podrían tomar, y plantear a las autoridades un plan para que de acá a 50 años no haya ardillas en la zona norte. Los modelos con los que voy a trabajar permiten predecir qué va a pasar con la población de ardillas en el futuro: qué va a pasar si no se hace nada y qué va a pasar si en cambio tomamos alguna medida para tratar de cercarla.

–¿Qué les contesta a quienes consideran estas investigaciones un sinsentido?

–Por empezar, la ecología es una rama científica con toda una metodología bastante rígida, en la que se tienen que seguir bastantes protocolos, hacer estudios sistemáticos y dedicarse un buen tiempo a estudiar, tomar datos, analizarlos e informarlos. Es posible que sea más fácil cuando se trata de un proyecto que tiene un resultado inmediato, que puede ser aplicable a algo, para resolver algún problema; eso es normalmente más fácil de entender. Pero toda la parte de investigación, donde es importante generar conocimiento, que tal vez después se pueda usar para aplicarlo a alguna cosa, en general mucho no se entiende. Lo importante consiste en reconocer que la ciencia también avanza al conocer, describir, entender y predecir.

Juegos de...

NUMEROS PRIMOS Y ASIMETRIA

La solución teórica fue encontrada casi simultáneamente en Inglaterra y Estados Unidos. Los especialistas británicos en cifrado, contratados por el gobierno, dieron con la respuesta antes, pero fue clasificada como *Top secret*, con lo cual quedó escondida por casi veinte años. Mientras tanto, de este lado del Atlántico, fueron dos tríos de investigadores quienes la consiguieron, y al no tener la obligación de mantenerla oculta la dieron a publicidad instantáneamente. Y más rápidamente aún, la patentaron.

En 1976, un grupo de investigadores de la Universidad de Stanford planteó la solución teóricamente: había que encontrar una función matemática que permitiera generar una clave asimétrica. Hasta ese momento, todas las claves criptográficas conocidas eran simétricas, lo que significa que se usaba el mismo código para cifrar y para descifrar el mensaje. En cambio, la clave asimétrica utiliza información diferente para codificar y decodificar el mensaje. Un año después, tres matemáticos del MIT (Massachusetts Institute of Technology) encontraron finalmente la solución. Ahora es conocida como "sistema RSA" por el nombre de sus autores: Ron Rivest, Adi Shamir y Leonard Adleman. Básicamente, consiste en una función en la que son importantes dos números primos (los que sólo pueden dividirse por uno y por sí mismos) a los que comúnmente se llama "p" y "q". La multiplicación de esos dos números genera "N".

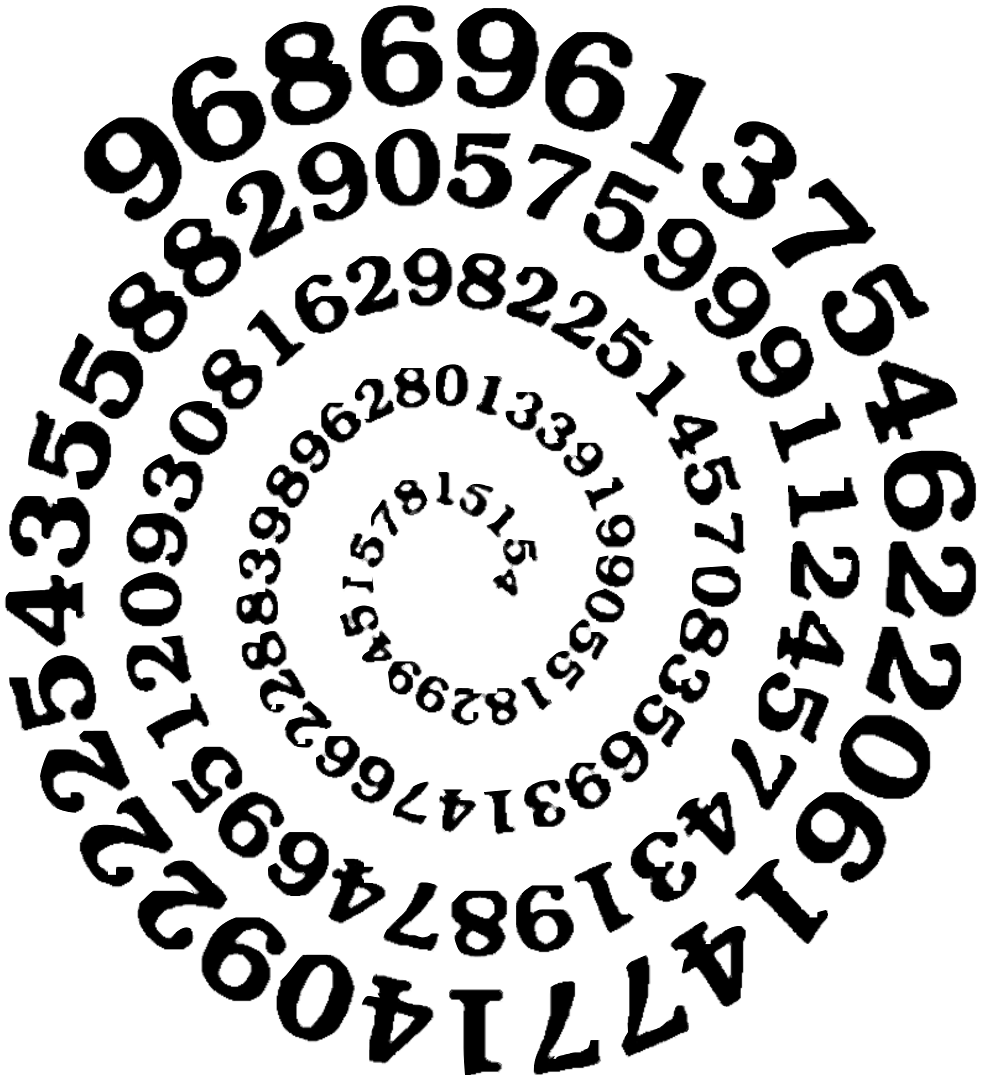
Supongamos que Andrés quiere enviarle un mensaje a Berta. Le pide a Berta su número "N" y lo utiliza para generar el texto cifrado. Para poder descifrarlo, no basta con conocer "N", hay que conocer "p" y "q", que Berta mantiene en secreto. Cualquiera que interceptara el mensaje de Andrés podría descifrarlo si encontrara "p" y "q", pero si el valor de "N" es lo suficientemente grande, eso podría llevarle mucho tiempo, porque tendría que probar hasta encontrar cuáles son los dos números primos que, multiplicados, dan "N". De esta manera, bastaría con enviarles a todos los capitanes de submarinos un solo número. Aunque el enemigo lo interceptara, le costaría décadas descubrir los dos números necesarios para descifrar el mensaje.

Los números "N" que se utilizan en las transacciones bancarias a través de Internet son tan grandes que los esfuerzos combinados de cien millones de computadoras tardarían más de mil años en descifrar "p" y "q". Este método recibe el nombre de cifrado con clave pública, justamente porque debe darse a conocer una parte de la clave para que los demás puedan codificar mensajes para uno.

La aparición de las computadoras personales agregó un nuevo factor: estas técnicas que sólo habían sido utilizadas por los estados o las empresas debido a los altos costos de las máquinas necesarias, estuvieron disponibles para los ciudadanos comunes.

PRIVACIDAD BASTANTE BUENA

En 1990, Philip Zimmerman, un físico y programador, creyó que ya era tiempo de que los ciudadanos comunes pudieran proteger su información del Estado, y desarrolló un programa llamado PGP (Pretty Good Privacy, que podría ser traducido como "Privacidad Bastante Buena") que permite crear un par de claves para cifrar archivos de computadora usando el sistema RSA. Mientras negociaba con los creadores de la fórmula la licencia para su utilización, el Congreso de los Estados Unidos estuvo a punto de prohibir el uso y exportación de softwares que permitieran la codificación de archivos. Antes de que todo su trabajo se echara a perder, Zimmerman decidió dar a conocer su programa, aunque todavía estuviera en desarrollo. Lo difundió en Internet y tuvo una enorme aprobación. Con esto se ganó dos grandes problemas: un juicio de los creadores del RSA y una investigación por parte del FBI por exportar "armas de guerra" sin autorización, categoría en la que habían caído los productos que contenían sistemas de cifrado complejos.


NUMEROS Y MAS NUMEROS. EL MENSAJE SECRETO DE RIVEST-SHAMIR-ADLEMAN (1977).

Después de tres años, y gracias a que el programa se difundió increíblemente por Internet y a que todavía no es fácil juzgar los delitos cometidos a través de la Red, el FBI decidió no llevarlo a juicio. La solución con los inventores del RSA fue más fácil, llegó a un acuerdo y pagó por la licencia.

LA SOCIEDAD DE LA INFORMACION

El enorme crecimiento de las comunicaciones digitales (Internet, la telefonía digital, por ejemplo) aumenta la importancia del cifrado inviolable. Toda la información que se convierte en ceros y unos puede ser codificada con el proceso RSA. Esto dificulta la investigación y el monitoreo que algunos estados llevan adelante. Si todas las comunicaciones digitales estuviesen cifradas, la red "Echelon" de espionaje comandada por Estados Unidos, Gran Bretaña y los países del Commonwealth perdería todo su poder.

Esta es la principal razón por la que los Estados están en contra de la proliferación de programas que faciliten el cifrado de mensajes. "Las organizaciones criminales serán imposibles de investigar", dicen como si esas organizaciones no tuvieran el dinero suficiente para pagar la creación de programas similares.

En 1998, 33 países reunidos en el Congreso de la Paz de La Haya, entre los que se encontraba Argentina, firmaron el acuerdo de Wassenaar, en el que se incluyó a las tecnologías de cifrado complejo dentro de las armas de guerra.

Por otro lado, los defensores de los derechos civiles dicen que todo el mundo tiene derecho a proteger sus documentos de los ojos indiscretos de los gobiernos. Hay Organizaciones No Gubernamentales especializadas en brindar asesoramiento en criptografía a otras organizaciones a lo largo y ancho del mundo.

Y, por último, están las empresas que necesitan de los programas de cifrado para aumentar la seguridad de las transacciones electrónicas y cuidar los datos de sus clientes a través de la Red. Además, las mismas empresas tienen miedo de que los Estados puedan inmiscuirse en sus comunicaciones y robar secretos que puedan ser usados en su contra. Por ejemplo, las comunicaciones entre la sucursal de una empresa alemana en Estados Unidos y su filial podrían ser interceptadas, y con la información obtenida ayudar a sus competidores norteamericanos.

La discusión está planteada y es de difícil solución. Los Estados quieren imponer regulaciones, mientras que las empresas y muchos ciudadanos ofrecen resistencia. A pesar de todo, la regulación de este tipo de programas ya parece una lucha perdida, tanto como la posibilidad de controlar la Web.

Después de los atentados a las Torres Gemelas, el gobierno norteamericano aumentó la presión, argumentando que con los sistemas criptográficos existentes los terroristas serían imposibles de investigar y, por lo tanto, jamás podrían reunir pruebas en su contra. Excusa bastante infantil, cuando ya demostraron que a falta de evidencias buenos son los informes de inteligencia. Y contra eso, hay poco en que los números primos puedan ayudar.


HOJA CON FILAS DE NUMEROS QUE LE FUERON ENCONTRADAS AL CHE GUEVARA AL SER CAPTURADO EN BOLIVIA.


UNA MENTE BRILLANTE. ALAN TURING (1912-1954).

TODOS LOS CAMINOS CONDUCEN A TURING

El gran matemático inglés Alan Turing (1912-1954) tuvo una participación importantísima en la Segunda Guerra Mundial, cuando el destino de los aliados se vio complicado por el ingenioso sistema de cifrado de la marina alemana, llamado Enigma, que parecía imposible de decodificar.

Como parte de sus investigaciones sobre los famosos axiomas de Euclides, Turing había estado trabajando en la posibilidad de que una máquina pudiese calcular. Desarrolló, primero teóricamente y luego lentamente en la práctica, un aparato que trabajaba en base dos (es decir, en código binario) y que, a partir de determinada información, podía tomar decisiones. O sea, lo que ahora llamamos computadora.

Mientras realizaba este trabajo, en 1938, fue visitado por Alistair Denniston, el encargado de la Escuela de Códigos y Cifras del Gobierno británico. Hacía tiempo que venían vigilando el accionar de Hitler e interceptando sus transmisiones que estaban cifradas con un código que resultaba esquivo. Alan Turing fue a Bletchley Park, lugar donde funcionaba el centro de descifrado de los ingleses. Empezó construyendo la máquina "Bomba", que permitió descifrar los mensajes de la fuerza aérea germana. El de la marina era una variación que llevó mucho más tiempo descubrir. Por fin en 1942 las comunicaciones de la marina alemana fueron leídas cotidianamente. Pero no tardaron en darse cuenta y mejorar su sistema, por lo que nuevamente los aliados fueron incapaces de entender los mensajes. En ese entonces comenzó el desarrollo del "Colossus", una computadora para descifrar mensajes. Evidentemente la computadora también nació como arma de guerra: faltaban dos años para que se desarrollara Eniac, la primera computadora de los Estados Unidos.

Turing fue condecorado con la Orden del Imperio Británico, medalla que no lo salvó, diez años después, cuando la policía se enteró por casualidad de la homosexualidad de Turing y lo detuvo. En el juicio posterior nunca negó su elección sexual y fue condenado a un año de prisión, que le fue condonado a cambio de un tratamiento con hormonas femeninas que le produjo terribles cambios en su cuerpo. Al poco tiempo se suicidó.

CRIPTOGRAFIA BASICA

◆ Todos los mensajes escritos pueden convertirse en cifras. Estas cifras pueden introducirse en una fórmula matemática codificable.

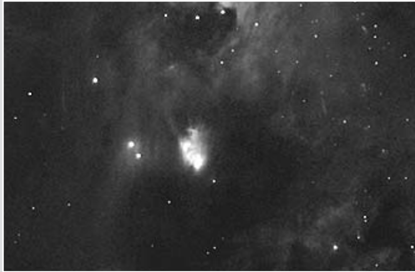
◆ En el sitio de Internet *www.pgpi.org* (una organización dedicada a la difusión internacional del PGP) puede encontrarse una explicación más detallada del funcionamiento de PGP, así como de otros proyectos, como el GnuPG, una solución similar de software libre que no utiliza ningún producto patentado.

◆ Como la legislación norteamericana prohíbe la exportación de los programas de cifrado sin una licencia del gobierno (lo que le otorga las herramientas para decodificar los mensajes), cuando sale una nueva versión del Pretty Good Privacy, la organización PGPi compra un libro que tiene el código, lo escanea y lo vuelve a compilar, logrando de esta manera hacerse del programa sin infringir las leyes norteamericanas (ya que no está prohibida la exportación de libros) e impidiendo que el gobierno de los Estados Unidos tenga acceso a la clave.

NOVEDADES EN CIENCIA

NEBULA A LA VISTA

ASTRONOMY En la época de los telescopios colosales, que adornan las grandes cumbres o las órbitas, como el magnífico Hubble, aún hay objetos en el cielo que escapan a la vista del más profesional y atento de los astrónomos. Así se entiende cómo la astronomía es una de las pocas ciencias donde todavía los aficionados –con medios mucho más precarios– desempeñan un papel activo e importantísimo, por ejemplo monitoreando la variabilidad de las estrellas, detectando cometas y descubriendo nuevas nébulas, como hizo el astrónomo amateur Jay McNeil la noche del 23 de enero en Kentucky (Estados Unidos) cuando apuntó su nuevo telescopio cerca de la constelación de Orión y fotografió una luminosa nube de gas y polvo, restos, según expertos, de una estrella en nacimiento, catalogada como IRAS 05436-0007.



Lo primero que este ahora famoso astrónomo amateur hizo después de ver lo que vio en el cielo, además de refregarse los ojos y saltar de alegría, fue llamar a su amigo Brian Skiff del Observatorio Lowell en Flagstaff, Arizona, quien confirmó el hallazgo.

Lo curioso es que la tímida nébula no aparece en ninguna de las colecciones astronómicas de objetos estelares que van de 1951 a 1991. Si bien otro astrónomo amateur, Evered Kreimer, la reportó en 1966, nadie se dignó a estudiarla, ni siquiera a catalogarla, y terminó siendo olvidada.

"Quedé absolutamente shockeado", confesó luego McNeil, instalador de antenas satelitales, y quien desde ahora puede alardear por el barrio de que hay un objeto a 1500 años luz de la Tierra que lleva su nombre: la nébula de McNeil, cerca del complejo nebuloso llamado M78 en la constelación de Orión.

EL MAR DE LOS MICROBIOS

Science Tal vez por asociación o por estar pegado a esa célebre (y tenebrosa) zona popularmente conocida como "Triángulo de las Bermudas", al Mar de los Sargazos, ubicado en el litoral de –justamente– las Islas Bermudas, no muchos se atreven a surcar (o al menos lo piensan dos veces y, antes de embarcar, se aseguran de despedirse de todos sus familiares). Lo cierto es que muchos aseguran no sólo haber encontrado allí la excusa perfecta para no subirse nunca más en su vida a un barco o a un botecito, sino también haber hallado 1800 especies nuevas de microbios, como acaba de anunciar el equipo de expertos en el genoma liderados por el multimediático Craig Venter, del instituto Celera Genomics.



Los científicos, que analizaron a los organismos diminutos en una muestra de agua y luego realizaron la secuencia del código genético, dieron con 1,2 millón de nuevos genes. "Al tomar muestras relativamente pequeñas de agua o suelo y usar las herramientas y técnicas del análisis de la secuencia podremos identificar y caracterizar las vastas legiones de organismos no vistos que viven en el ambiente", dijo el siempre simpático Venter, jefe también del Instituto de Alternativas de Energía Biológica, en Maryland, Estados Unidos.

Lo más sorprendente, aseguran, fue el descubrimiento de 800 nuevos genes para fotorreceptores, unas estructuras usadas por las criaturas marinas para captar la luz. Hasta ahora, sólo 150 genes fotorreceptores habían sido hallados entre todas las especies conocidas.

"Nuestro trabajo en el Mar de los Sargazos, un área que se pensaba tenía una escasa diversidad de especies, ha revelado mucho de lo que aún no se entendía sobre el océano y sus habitantes", expresó Venter, cuya cuenta bancaria crece día a día.

NOVEDADES MARCIANAS

◆ Científicos de la Agencia Espacial Europea (ESA) aseguran que el Beagle 2, la sonda cuya misión era buscar indicios de vida en Marte, se habría estrellado al entrar al planeta rojo el 25 de diciembre pasado debido a que la atmósfera era menos densa de lo que se esperaba. Hasta ahora se creía que el robot se había posado en la superficie y que por alguna razón desconocida no enviaba señales a la sonda Mars Express que orbita el planeta. También el responsable del robot, Colin Pillinger, cree que el vehículo que llevaba en su interior al Beagle 2 se precipitó a alta velocidad, y los airbags no pudieron soportar la dureza del choque contra Marte.



◆ A menos de una semana de que los ingenieros de la NASA afirmaran que el robot Opportunity encontró vestigios de agua líquida en el rocoso y polvoriento suelo marciano, su gemelo, el Spirit, en el otro lado del planeta (cráter Gusev) halló también indicios de que ciertas zonas de Marte fueron ambientes húmedos, aunque de momento no se sabe si pudo haber vida. Así lo dedujeron los científicos de la NASA tras analizar información extraída por el Spirit de una roca volcánica oscura bautizada "Humphrey". Sin embargo, la cantidad de agua con la que esta roca estuvo alguna vez sería mucho menor que la que habría habido en Meridiani Planum, por donde en este momento se desplaza el Opportunity.

◆ El lunes pasado, en su "sol 64", el Spirit alcanzó la marca de los 300 metros de distancia desde su llegada a Marte, el 5 de enero.

◆ Del otro lado del planeta, el Opportunity posó sus instrumentos de abrasión y su espectrómetro Moessbauer en la roca "Mojo 2". También tomó con sus cámaras panorámicas fotografías tridimensionales del área bautizada "Berry Bowl" e hizo mediciones atmosféricas con su espectrómetro de emisión termal.

◆ La NASA anunció el miércoles que tanto el Spirit como el Opportunity podrán quedarse en Marte 240 días, más de 150 de los que se habían planeado originalmente, dado que los ingenieros estadounidenses concluyeron que el consumo de energía de los aparatos resultó ser menor del previsto.

LIBROS Y PUBLICACIONES

EL RETO DE HILBERT: LOS 23 PROBLEMAS QUE DESAFIARON A LA MATEMÁTICA
Jeremy J. Gray
Drakontos
Crítica-Planeta, 343 pp.



La figura de David Hilbert presidió la matemática de las primeras décadas del siglo XX, por lo menos de manera programática, ya que Hilbert, en cierta forma parecido a Gauss, incursionó en todos los rincones de la ciencia de las ciencias. *El reto de Hilbert* da buena cuenta de la trayectoria del gran David y sus logros, centrándose en los famosos 23 "problemas pendientes" que presentó en el Congreso Internacional de Matemáticas de París en el año 1900. Eran épocas de ascenso irresistible –bien adentro del paradigma del progreso– en las que parecía que el rigor y una axiomática adecuada no sólo sostendrían el edificio entero, sino que además le permitirían expandirse ilimitadamente.

No fue así: en 1931, Gödel demostró que el programa "demostrémoslo todo" era imposible, por lo menos visto desde al ángulo de la lógica matemática, e inauguró una era de discusiones fecundas que sacudieron no sólo las matemáticas sino la filosofía y que pusieron un rico epílogo a la "crisis de los fundamentos", de alguna manera inaugurada con la irrupción de las geometrías no euclidianas en el siglo XIX (y continuada por Cantor), crisis que, preciso es decirlo, no afectó demasiado el "desarrollo normal" de la disciplina, para utilizar la terminología kuhniana. Así, *El reto de Hilbert* recorre los avatares matemáticos de la primera mitad del siglo XX a través del ambicioso programa de Hilbert de 1900.

El reto de Hilbert es un libro interesante y que vale la pena, aunque es necesario advertir que es bastante técnico, y quienes no son matemáticos, o no tienen cierta formación matemática tendrán dificultades. Al fin y al cabo, los famosos 23 problemas no eran precisamente fáciles. **L.M.**

CAFE CIENTIFICO

EXTRATERRESTRES
Organizado por el Planetario, el martes 16 de marzo a las 18.30 comienza un nuevo ciclo de Café Científico que se muda este año al **Hotel Bauen**, Av. Callao 360. El título del primer encuentro es "¿Y si no estamos solos?: Vida extraterrestre". Expondrán Sergio Parón (físico, investigador del IAFE) y Miguel de Asúa (titular de Historia de la ciencia, Esc. de posgrado, Univ. San Martín). Gratis.

AGENDA CIENTIFICA

DIVULGACION CIENTIFICA
El martes 13 de abril comienza el curso de "Introducción a la divulgación científica" que ofrece la Facultad de Ciencias Exactas de la UBA. Destinado a docentes, graduados y estudiantes avanzados, de ciencia o de comunicación. Informes: *sgallardo@bl.fcen.uba.ar*

MENSAJES A FUTURO
futuro@pagina12.com.ar

CICLO DE CAFE CIENTIFICO, VERSION 2004

El café de la victoria (científica)

POR LEONARDO MOLEDO



Cuando en 1683 los turcos se retiraron levantando el sitio de Viena –aceptó Solimán el Magnífico su derrota– dejaron equipaje y provisiones, entre las que se contaban numerosas bolsas de café, que sirvieron para que funcionara La botella Azul, el primer café vienés, que inauguraría una moda en Europa y produjo delicias como la *Cantata del Café* de Johann Sebastian Bach. Lo demás es historia conocida: el café como lugar de reunión, el cafetín como inspiración del tango y discutible universidad del barrio; el café como refugio de la bohemia, y ahora, al compás del nuevo milenio, el producto más sofisticado, si se quiere, de la planta que mantiene despierta a media humanidad y provoca acidez al resto: el café científico.

En el año 2001, cuando se produjo la debacle argentina, el fenómeno de las fábricas y empresas recuperadas –obreros y empleados que ponían a funcionar aquello que sus dueños abandonaron– se constituyó en una solución original y novedosa (de la que da cuenta magníficamente Esteban Magnani en su libro *El cambio silencioso*), de las cuales Zanon, Brukman o el Hotel Bauen son verdaderos ejemplos.

Ahora, en el año 2004 el producto más sofisticado del café (el café científico) y el producto más nuevo de la sociedad argentina tratando de recuperarse (la empresa recuperada Bauen, que justamente en alemán significa construir) se unen para dar continuidad al ciclo de charlas gratuitas ("Cafés Científicos") que desde el año 2001 organiza el Planetario de la Ciudad de Buenos Aires, con una respuesta masiva, y que el martes próximo a las 18.30 volverá al ruedo en las instalaciones del Hotel Bauen (Avda. Callao 360).

Como siempre, el café científico es el lugar en el que la ciencia discurre; en donde ninguna pregunta es impertinente y el contacto cara a cara con el científico argentino de turno se estrecha, entablando un diálogo ameno y cordial como uno puede tener con el vecino o con el compañero de trabajo.

Aunque la incitativa del Planetario Galileo Galilei fue independiente, se realizan cafés científicos en otras ciudades del mundo: en Lyon, en Londres, en Oxford (Coffee Republic, Blackwells Main Bookshop, Broad Street, Oxford), Lyon, Brest, Caen, Montpellier, Nantes, París, Montreal (Canadá), Kobenhaven (Dinamarca), Rabat (Marruecos), Ginebra (Suiza) y muchas más; la página de Internet donde figura la lista completa está en *www.cafescientifique.org*. No parece haber café científico en Addis Abeba, Etiopía, la patria del café, ni en Colombia, ni en Brasil. Participar, así, en un café científico, no es solamente sumirse en la conversación, escuchar la ciencia contada (la ciencia es ciencia solamente cuando se cuenta, cuando se comunica, no cuando queda olvidada en los laboratorios), no es solamente engancharse en la tradición que comenzó con La botella azul, o con el movimiento de empresas recuperadas, sino también participar de una extensa red que reúne a muchas ciudades del mundo, donde la gente quiere conocer lo que los científicos conocen, y que los científicos conozcan las ideas y las dudas de quienes no son especialistas en tal o cual tema.

LOS TEMAS DEL CUARTO CICLO DE CAFÉ CIENTÍFICOS SON:

◆ **16 de marzo: ¿Y si no estamos solos?** Vida extraterrestre.
◆ **20 de abril: Temblores.** ¿Puede haber terremotos en Buenos Aires?
◆ **18 de mayo:** Cometas. Apariciones y curiosidades de las "estrellas con cabellera".
◆ **15 de junio: Cero absoluto: cuando nada se mueve.** Superconductividad y bajas temperaturas.
◆ **20 de julio: ¿Se puede confiar en los pronósticos?** Los caprichos del tiempo.
◆ **24 de agosto: Psiquiatría versus psicología.** Medicación o terapia.
◆ **21 de septiembre: Sociobiología: homicidio.** ¿Por qué la gente mata?
◆ **19 de octubre: Música y ciencia: estridencias.** ¿Por qué los instrumentos suenan como suenan?
◆ **16 de noviembre: Veo multitudes.** Superpoblación, crecimiento humano y extinciones.

FINAL DE JUEGO / CORREO DE LECTORES

Donde se habla sobre una inconsistencia y se plantea un enigma con cumpleaños

POR L. M.

–Bueno –dijo Kuhn–, estoy contento porque el martes próximo empieza el ciclo de Cafés Científicos de este año.
–Y sobre Vida Extraterrestre –dijo el Comisario Inspector–. No está mal para empezar. Y además, se hace en el Hotel Bauen (Cooperativa de trabajo, en Callao 360, casi esquina Corrientes), una empresa recuperada que, como todo el mundo sabe, goza del afecto de la policía.
–Nadie contestó el enigma de la semana pasada –dijo Kuhn.
–Qué notable –dijo el Comisario Inspector–. Y eso que era un enigma fácil. La pregunta era si la frase "yo estoy en contra de todo" era consistente.
–¿Y es consistente?
–Parece que no –dijo el Comisario Inspector–, porque si fuera consistente, una persona que está en contra de todo estaría en particular en contra de estar en contra de todo y, por lo tanto, habría algo contra lo cual no está. De donde se deduce que no está en contra de todo, *quod erat demostrandum*.
–Latinajos –dijo Kuhn–. Mirando la hora, yo diría que deberíamos pasar al enigma.
–Veo que ya no son problemas de espacio, planteados por nuestro diagramador demente (por estas semanas reemplazado por otro diagramador demente, Luis, que se va a trabajar a Barcelona), sino de tiempo –dijo el Comisario Inspector–, lo cual muestra que este asunto relativista de las cuatro dimensiones ha calado profundamente en este diario.
–Ahora dicen los cosmólogos que las dimensiones originarias eran como dieciséis, y que todas menos cuatro se arrollaron –dijo Kuhn–. Pero no lo creo... Ni siquiera sé qué significa que "se arrollaron".
–Yo tampoco creo esas cosas –dijo el Comisario Inspector–, aunque a veces pienso en un tiempo de dos dimensiones, que ofrece muchas posibilidades interesantes. Algún día podríamos hablar de eso, pero ahora vamos al enigma, que es éste: al Jefe de Policía le gusta hacer preguntas sucesivas para averiguar el día de nacimiento de una persona. Por ejemplo: –él es supersticioso– ¿de qué signo es usted? Y luego, ¿cerca de tal otro signo o del de más allá? Y así. Hasta ahora, ha logrado un sistema de catorce preguntas que permiten averiguarlo. Hay un comisario, por otra parte, que hace lo mismo pero sólo con trece preguntas. El enigma es: ¿cuál es el mínimo de preguntas que se puedan contestar sí o no necesarias para averiguar el cumpleaños de una persona?

¿Qué piensan nuestros lectores? ¿Cuál es el mínimo de preguntas? ¿Y van a venir al Café Científico en el Bauen?

Correo de lectores

CRITICA BIENVENIDA

Estimado Leonardo: Nunca agradecí la crítica a "Somos nuestro cerebro", ya que me quedé con la duda de si debía o no hacerlo, por eso de mantener la independencia de los críticos, etc. Pero, bueno, ya que estoy me encantó y puedo decir que nos "sacaste la ficha" perfecta. Muchas gracias.

El tema de este mail sin embargo es por la nota de Alicia Marconi sobre los trastornos de ansiedad del penúltimo nº de **Futuro**. La verdad, me produjo preocupación.

Coincido con Marconi en la necesidad de darle una discusión más amplia al tema que lo surgido de la investigación de la gente del NIMH. Los trastornos de ansiedad (TA) son un grupo de trastornos causan enormes sufrimientos a muchas personas, pero tienen un difuso borde con la normalidad y al mismo tiempo son blanco de enormes intereses comerciales. (...) Marconi se "alegra" de que las cosas no sean "tan así" y que la psicoterapia tenga un lugar. Es prejuiciosa y plantea una antinomia que no existe. Hace rato que no estamos pensando en "Pastillas vs. Psicoterapias" y poner a los pacientes en esa posición solo lleva a tironeos y desmembramientos.

Finalmente Marconi consulta a un profesional para dar base a lo que fue su intención de entrada: relativizar y criticar lo que supuestamente iba a informar (...) (y) la analista consultada (a la cual sinceramente imagino de buen nivel por sus dichos) desliza una serie de hipótesis causales del trastorno que están muy, pero muy lejos de estar probadas. Para coronar el asunto, la emprende con una aseveración político-ideológica sobre los orígenes de los TA adjudicándoselos a la globalización y señalando a la medicación como un instrumento de sobreadaptación. (...)

Este tipo de visiones ideológicas sobre la salud de las personas solo aumentan el estigma y empeoran las posibilidades de acceso a tratamiento. (...)

Saludos de un lector de siempre y gracias por todo.

Sergio Strejilevich